NICE-PAKE: On the Security of KEM-Based PAKE Constructions without Ideal Ciphers

Nouri Alnahawi[1,4], Jacob Alperin-Sheriff[2], Daniel Apon[3], and Alexander Wiesmaier[1,4]

[1] Hochschule Darmstadt. {nouri.alnahawi,alexander.wiesmaier}@h-de.de
[2] Independent Researcher. jacobmas@gmail.com
[3] The MITRE Corporation. crypto@mitre.org
[4] National Research Center for Applied Cybersecurity ATHENE.

Abstract. The interest in realizing generic PQC KEM-based PAKEs has increased significantly in the last few years. One such PAKE is the CAKE protocol, proposed by Beguinet et al. (ACNS '23). However, despite its simple design based on the well-studied PAKE protocol EKE by Bellovin and Merritt (IEEE S&P '92), both CAKE and its variant OCAKE do not fully protect against quantum adversaries, as they rely on the Ideal Cipher (IC) model. Related and follow-up works, including Pan and Zeng (ASIACRYPT '23), Dos Santos et al. (EUROCRYPT '23), Alnahawi et al. (CANS '24), and Arragia et al. (IACR '24/308) although touching on that issue, still rely on an IC. Considering the lack of a quantum IC model and the difficulty of using the classical IC to achieve secure instantiations on public keys in general and PQC in particular, we set out to eliminate it from PAKE design. In this paper, we present the **N**o **IC** **E**ncryption (**NICE**)-**PAKE**, a (semi)-generic PAKE framework providing a quantum-safe alternative for the IC, utilizing simpler cryptographic components for the authentication step. To give a formal proof for our construction, we introduce the notions of A-Part-Secrecy (A-SEC-CCA), Splittable Collision Freeness (A-CFR-CCA) and Public Key Uniformity (SPLIT-PKU) for splittable LWE KEMs. We show the relation of the former to the Non-uniform LWE and the Weak Hint LWE assumptions, as well as its application to ring and module LWE. Notably, this side quest led to some surprising discoveries, as we concluded that the new notion is not directly interchangeable between the LWE variants, or at least not in a straightforward manner. Further, we show that our approach requires some tedious tweaking for the parameter choices in both FrodoKEM and CRYSTALS-Kyber to obtain a secure PAKE construction. We also address some fundamental issues with the common IC usage and identify differences between lattice KEMs regarding their suitability for generic PQC PAKEs, especially regarding the structure of their public keys. We believe that this work marks a further step towards achieving complete security against quantum adversaries in PQC PAKEs.

Keywords: Password Authenticated Key Exchange · PAKE · Key Encapsulation Mechanism · KEM · Post-Quantum Cryptography · PQC · Learning with Errors · LWE · Ideal Cipher Model · IC